Gegevensbeschermingsbeleid

van

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V.

gevestigd te Leek

In verband met de Algemene Verordening Gegevensbescherming
Ingangsdatum: 25 mei 2018

Inhoudsopgave

1. Inleiding

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (of General Data Protection Regulation) rechtstreeks van toepassing in alle lidstaten van de Europese Unie. Deze verordening is de opvolger van de Wet bescherming persoonsgegevens in Nederland. Het doel van de Verordening is om twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie ('EU').

De Verordening heeft rechtstreekse werking binnen de gehele Europese Unie en harmoniseert daarmee de regels voor de bescherming van persoonsgegevens. Maar, op specifieke punten biedt de Verordening lidstaten de ruimte om nadere invulling te geven aan de bepalingen. Deze invulling geschiedt via zogenaamde uitvoeringswetten. Dit document is geschreven vanuit het perspectief van de Nederlandse Uitvoeringswet. Houd er rekening mee dat afhankelijk van uw specifieke situatie niet de Nederlandse, maar een andere uitvoeringswet op uw gegevensverwerkingen van toepassing kan zijn. De inhoud daarvan kan afwijken van hetgeen in dit document is beschreven.

De verordening is een omvangrijk stuk wetgeving met slechts een beperkte schriftelijke toelichting. Op veel punten is het daarom (nog) onduidelijk wat de precieze invulling is die gegeven moet worden aan begrippen en bepalingen. Omdat de verordening een Europese wet is waarvan de verdere invulling aan de toezichthouder(s) en de Europese rechter is, wordt in deze handleiding slechts zeer beperkt vooruitgelopen op de interpretatie van nu nog onduidelijke begrippen. Daar waar er in het bijzonder onduidelijkheid is over de invulling en interpretatie van begrippen wordt dit expliciet vermeld.
Dit document kan in het licht van het bovenstaande periodiek herzien worden om de laatste ontwikkelingen op het gebied van de toepassing en de uitleg van de verordening mee te nemen.

Dit document is bedoeld als intern beleidsdocument voor Boomzagerij- Boomrooierij-Rondhouthandel Sikko Polling B.V., ongeacht de handelsnaam waaronder ze opereert, en daaraan verbonden ondernemingen en deelnemingen. Dit document is samengesteld door het bestuur in samenspraak met door het bestuur aangetrokken juridische adviseurs. Dit document is bedoeld voor iedereen binnen de organisatie die meer wil of moet weten over de AVG.

2. Bedrijfsomschrijving

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. is opgericht op 1 maart 1984. Sinds de oprichting houdt de onderneming. zich bezig met de boomzagerij, boomrooierij en rondhouthandel.

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. is ingeschreven bij de Kamer van Koophandel onder nummer 72320869.

3. Gegevensverwerking en verantwoordelijkheid

Inleiding
De verordening geeft aan welke handelingen met persoonsgegevens worden beschouwd als ‘verwerkingen’. Een verwerking is volgens de verordening elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens.

Veel voorkomende bewerkingen zijn:
- het verzamelen van persoonsgegevens;
- het vastleggen van persoonsgegevens;
- het opslaan van persoonsgegevens;
- het wijzigen van persoonsgegevens;
- het opvragen van persoonsgegevens;
- het raadplegen van persoonsgegevens;
- het gebruiken van persoonsgegevens;
- het verstrekken van persoonsgegevens;
- het wissen en vernietigen van persoonsgegevens.

In de praktijk komt het er dus op neer dat een verwerkingshandeling al snel een verwerking van persoonsgegevens in de zin van de verordening is.

De verordening is echter niet van toepassing op de verwerking van alle soorten gegevens, maar alleen op de verwerking van persoonsgegevens.
Persoonsgegevens zijn alle gegevens die:
1. betrekking hebben op;
2. een geïdentificeerde, of;
3. identificeerbare;
4. natuurlijke persoon.

De gegevens van rechtspersonen zijn geen persoonsgegevens. De gegevens van de contactpersonen van die rechtspersonen zijn wel persoonsgegevens. De natuurlijke persoon op wie de gegevens betrekking hebben wordt de ‘betrokkene’ genoemd.

Op grond van het vorenstaande kwalificeert Sikko Polling B.V. als een verwerker van persoonsgegevens en is daarom onderworpen aan de regelgeving van de verordening. Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. is verwerkingsverantwoordelijk in de zin van de verordening.

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. wordt in de vorm van een besloten vennootschap (B.V.) gedreven en is daarom als rechtspersoon de verwerkingsverantwoordelijke, niet de individuele werknemer die het besluit heeft genomen om persoonsgegevens te verwerken. Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. heeft als rechtspersoon de formeel-juridische bevoegdheid tot het nemen van beslissingen.

4. De wijze van verkrijging van persoonsgegevens

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. verwerft op diverse manieren persoonsgegevens, waaronder handmatige invoer door bestuurders, naar aanleiding van contact met betrokkenen, afgifte van visitekaartjes, door een telefonische intake, door een bestelling per telefoon of per e-mail, een bestelformulier, cookies op de website etc.

Externe bronnen
Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. verzamelt incidenteel persoonsgegevens uit externe bronnen. Daarbij kan gedacht worden aan (algemene) contactgegevens via een website of via google.

Relaties en persoonsgegevens

- de onderneming levert diensten aan consumenten (B2C), maar ook aan bedrijven en organisaties (B2B) indien zij werkzaam zijn als onderaannemer.
- de onderneming koopt zaken en diensten in van bedrijven en organisaties (B2B).
- De persoonsgegevens hebben betrekking op potentiële, bestaande of oude klanten en leveranciers.
- de onderneming verwerkt persoonsgegevens op geautomatiseerde wijze, wat wil zeggen dat zij met behulp van één of meerdere computers persoonsgegevens opslaat, bewerkt, etc. Met andere woorden: de klantadministratie en leveranciersadministratie wordt digitaal beheerd.
- de onderneming verwerkt géén bijzondere persoonsgegevens.
- De persoonsgegevens zijn afkomstig van de klanten of de leveranciers zelf, de onderneming heeft ze niet van derden gekocht.
- De gegevens worden niet gekoppeld aan of samengevoegd met andere gegevens van de klant of leverancier die op een ander moment en/of in een andere context zijn verkregen, waardoor de onderneming nog meer weet van de desbetreffende personen.
- Bij de verwerking van persoonsgegevens maakt zij verder geen gebruik van (volledig) nieuwe technologie (bijv. vingerafdruksystemen of gezichtsherkenning).
- Daarnaast komen de verwerkingen niet neer op het volgen van de locatie of de verplaatsingen van personen.
- de onderneming stelt met behulp van de persoonsgegevens geen profielen op van de betrokkenen om een beeld te krijgen van bijvoorbeeld hun interesses, gedrag of economische situatie, en dergelijke.
- de onderneming verstrekt de persoonsgegevens van haar klanten en leveranciers alleen aan andere leveranciers en opdrachtnemers in het kader van het uitbesteden van werkzaamheden en het inkopen van zaken zoals materialen, onderdelen en eindproducten.
- de onderneming doet aan direct marketing.
- de onderneming communiceert met haar (potentiële) klanten en leveranciers en sluit overeenkomsten met hen per e-mail, schriftelijk en telefonisch.
- Opslag van persoonsgegevens bij Sikko Polling B.V. vindt plaats op de harde schijf van de eigen computer(s), bij haar zelf aanwezige extra schijfruimte en bij cloud diensten.
- de onderneming maakt daarnaast gebruik van de diensten van een hosting-/cloudprovider. Deze provider levert opslagruimte en host de bedrijfswebsite en e-mail. Voor diverse boekhoudprogramma's wordt ook gebruik gemaakt van cloud oplossingen.

5. Legitimiteit van de verwerking

Inleiding
De AVG verordening stelt dat de verwerking van persoonsgegevens rechtmatig, behoorlijk en transparant zijn moet. Op grond van de verordening en de daaraan gegeven uitleg heeft Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. nader onderzoek naar de persoonsgegevens die zij verwerkt en of deze verwerking overeenkomt met de verplichtingen uit de verordening.
De onderneming heeft de navolgende beginselen beoordeeld:

1. Doelbinding
De verwerking moet gebonden zijn aan specifieke verzameldoelen ("doelbinding"). Persoonsgegevens mogen alleen worden verzameld en verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Wanneer de gegevens later voor een ander doel worden gebruikt, dan moet dat nieuwe doel verenigbaar zijn met het oorspronkelijke verzameldoel.

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. gebruikt de persoonsgegevens die zij verwerkt voor geen andere doeleinden dan waarvoor zij die gegevens heeft verzamelt dan wel heeft ontvangen en overeenkomstig het doel waarvoor deze gegevens zijn verstrekt.

2. Minimale gegevensverwerking
Wanneer persoonsgegevens worden verwerkt dan moeten zij voor het doel toereikend en ter zake dienend zijn. Verder mogen er niet meer persoonsgegevens worden verwerkt dan noodzakelijk voor het doel. Met andere woorden, er mogen gelet op het doel, niet te veel, maar ook niet te weinig gegevens worden verwerkt voor het doel. Wanneer u namelijk te weinig gegevens verwerkt, dan kan er ten onrechte een onvolledig beeld ontstaan van de betrokkene.

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. verzamelt de persoonsgegevens met zorg en heeft aandacht besteed aan deze voorwaarde.

3. Juistheid
De verwerkingsverantwoordelijke moet alle redelijke maatregelen nemen om ervoor te zorgen dat de gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn, dienen te worden gewist of gecorrigeerd. Hierbij dient ook rekening te worden gehouden met de ontvangers van persoonsgegevens.

4. Opslagbeperking
Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel van de verwerking. Wanneer de gegevens niet langer noodzakelijk zijn, dan moeten zij worden vernietigd of gewist.

5. Integriteit en vertrouwelijkheid
Persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. is verantwoordelijk voor de naleving van deze beginselen en moet ook kunnen aantonen dat een verwerking van persoonsgegevens aan de hiervoor bedoelde beginselen voldoet. Voor zover daar in deze paragraaf geen concrete uitspraken zijn gedaan voldoet Sikko Polling B.V. hieraan onder meer door een register van verwerkingsactiviteiten bij te houden. Ook overige maatregelen zijn opgenomen in dit document.

Verwerkingen die plaats vonden, maar waarvoor binnen de AVG geen legitimiteit geldt, zijn gestaakt.

6. Informatievoorziening aan betrokkenen

Inleiding
Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. neemt als uitgangspunt dat zij altijd een informatieplicht heeft wanneer zij persoonsgegevens verwerkt. Met betrekking tot het informeren van de betrokkene maakt de verordening echter een onderscheid tussen twee situaties:

- de gegevens worden bij de betrokkene zelf verzameld; en
- de gegevens worden buiten de betrokkene om verkregen.

Zoals hiervoor aangegeven verzamelt Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. in de meeste gevallen de gegevens rechtstreeks bij de betrokkene. In enkele gevallen kunnen ook gegevens buiten de betrokkene om verkregen worden, bijvoorbeeld via andere personen of organisaties of omdat ze op het internet staan.

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. informeert betrokkenen als de gegevens voor een ander doel gebruikt gaan worden dan waar ze oorspronkelijk zijn verzameld.

Beleid
In verband met het hiervoor genoemde onderscheid heeft Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. het navolgende beleid:

1. Verzameling van gegevens bij de betrokkene zelf
Wanneer de onderneming de gegevens bij de betrokkene zelf verzamelt, dan wordt de volgende informatie verstrekt:

- de identiteit van de onderneming en haar contactgegevens;
- indien een functionaris voor de gegevensbescherming wordt aangesteld, de contactgegevens van deze functionaris;
- de doelen waarvoor de persoonsgegevens worden verwerkt;
- de grondslag waarop de verwerking is gebaseerd;
- voor zover van toepassing: wanneer de verwerking wordt gebaseerd op de grondslag ‘gerechtvaardigd belang’: wat dit gerechtvaardigd belang is;
- de eventuele ontvangers of categorieën ontvangers van de gegevens;
- in geval van verstrekking aan derde landen:
  - ✓ of er een adequaatheidsbesluit van de Commissie bestaat;
  - ✓ of passende waarborgen zijn getroffen, welke dit zijn en of hier een kopie van kan worden verkregen, dan wel waar die waarborgen kunnen worden geraadpleegd;
- de bewaartermijn, of als dat niet mogelijk is de criteria voor het bepalen ervan;
- de rechten van de betrokkene;
- in het geval van toestemming, dat de betrokkene die toestemming altijd weer kan intrekken;
- dat de betrokkene het recht heeft een klacht in te dienen over onze verwerking bij de Autoriteit Persoonsgegevens;
- of het verwerken van persoonsgegevens een wettelijke verplichting is of noodzakelijk is voor de uitvoering of het aangaan van een overeenkomst, of de betrokkene verplicht is die gegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken van die gegevens voor de betrokkene;
- in geval van geautomatiseerde besluitvorming, nuttige informatie over de onderliggende logica, het belang van de verwerking en de verwachte gevolgen van die verwerking voor de betrokkene.

Verder moet alle andere informatie worden verstrekt die noodzakelijk is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen. Sikko Polling B.V. heeft de conclusie getrokken dat geen nadere informatievoorziening noodzakelijk is naast het opstellen van een privacy statement en cookie statement die zijn gepubliceerd op de website.

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. zal de betrokkenen opnieuw informeren als de persoonsgegevens voor andere doelen verder worden verwerkt, voor zover de betrokkene nog niet van die informatie op de hoogte is.

2. Verkrijging van gegevens buiten de betrokkene om

Wanneer Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. gegevens verzamelt buiten de betrokkene om zal de bron worden toegevoegd waaruit de persoonsgegevens zijn verkregen. In de gevallen dat de bron niet kan worden vastgesteld zal Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. algemene informatie over de herkomst verstrekken.

Informatieplicht huidige klanten

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. heeft haar huidige klanten na intreding van de AVG middels haar privacy statement geïnformeerd. Dit privacy statement heeft zij per e-mail aan haar klanten verzonden en is publiek toegankelijk op de website. Het privacy statement van Sikko Polling B.V. is bijgevoegd als **bijlage**.

Informatieplicht nieuwe klanten

Nieuwe klanten sluiten een overeenkomst met de onderneming. In deze overeenkomst wordt de klant/betrokkene gewezen op de persoonsgegevens die worden verwerkt en de reden van verwerking. Bij deze informatievoorziening wordt de klant/betrokkene gewezen op de inhoud van het privacy statement.

7. Rechten van betrokkenen

Inleiding
Betrokkenen hebben onder de AVG rechten ten aanzien van hun persoonsgegevens. Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. is verplicht betrokkenen te informeren over hun rechten (artikel 13 en 14 van de AVG). De onderneming heeft hiervoor een privacy statement opgesteld.

Ook moet de onderneming in staat zijn om adequaat te kunnen reageren op een betrokkene die één van zijn rechten wenst uit te oefenen. Een betrokkene heeft de volgende rechten:

1. Recht van inzage (artikel 15 AVG);
2. Recht op rectificatie (artikel 16 AVG);
3. Recht op vergetelheid (gegevenswissing) (artikel 17 AVG);
4. Recht op beperking van de verwerking (artikel 18 AVG);
5. Recht op dataportabiliteit (overdraagbaarheid gegevens) (artikel 20 AVG);
6. Recht van bezwaar tegen verwerking (artikel 21 AVG);

Betrokkenen hebben dus het recht om na te gaan wat er met hun persoonsgegevens gebeurt (punt 1) en hier als dit nodig is invloed op uit te oefenen (punt 2 t/m 6).
De informatieplicht hangt daarmee nauw samen met de rechten van betrokkenen: aan de ene kant is er de verplichting voor Sikko Polling B.V. om betrokkenen actief, tijdig en adequaat te informeren over verwerkingen van persoonsgegevens; aan de andere kant kunnen betrokkenen hun rechten uitoefenen richting Polling Vastgoed.

Ten behoeve van de feitelijke uitvoering is als **bijlage** het protocol ‘Protocol uitvoering rechten betrokkenen’ ingevoegd. In dit protocol is uitgewerkt wat de voormelde rechten van betrokkenen inhouden en hoe Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. met verzoeken van betrokkenen omgaat.

8. De (sub)verwerkers en de verwerkersovereenkomsten

Inleiding
Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. maakt gebruik van diverse verwerkers. Een verwerker is de partij die voor Sikko Polling B.V. persoonsgegevens verwerkt. Op basis van de verordening zal Polling Vastgoed, bij gebruik van verwerkers, de verwerking door die verwerker moet regelen in een verwerkersovereenkomst of anderszins bindende rechtshandeling.

De verwerkersovereenkomst dient in schriftelijke vorm, waaronder elektronische vorm, te worden opgesteld.

De verwerkers waar de onderneming zaken mee doet zijn per afzonderlijke onderneming opgenomen in het register van verwerkingsactiviteiten.
Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. heeft met de aan haar verbonden verwerkers een verwerkersovereenkomst gesloten of zal deze sluiten.

Een aantal van de verwerkers heeft de voorwaarden van haar dienstverlening, en de verplichtingen die voortvloeien uit de AVG, vastgelegd in haar verwerkingsvoorwaarden (Data Processing Terms of Data Processing and Security Terms).

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. heeft met de aan haar verbonden verwerkers en verwerkingsverantwoordelijken verwerkersovereenkomsten gesloten dan wel zal een dergelijke overeenkomst sluiten. In die verwerkersovereenkomsten zullen in ieder geval de volgende zaken worden vermeld:

- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.

Verder dient in de verwerkersovereenkomst te worden bepaald dat de verwerker:
- de persoonsgegevens alleen verwerkt onder de schriftelijke instructies van de verwerkingsverantwoordelijke, onder andere voor wat betreft de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie (tenzij deze daartoe wettelijk is verplicht);
- waarborgt dat de toegang tot die gegevens is beperkt tot gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting;
- minimaal hetzelfde niveau van beveiliging van de persoonsgegevens hanteert als de verwerkingsverantwoordelijke;
- de verwerkingsverantwoordelijke alle mogelijke ondersteuning biedt bij het nakomen van diens verplichtingen met het oog op de beantwoording van verzoeken rondom de rechten van betrokkenen;
- de verwerkingsverantwoordelijke bijstaat bij het nakomen van diens verplichtingen op het gebied van de beveiliging van persoonsgegevens en de meldplicht datalekken;
- na beëindiging van de overeenkomst de in opdracht van de verwerkingsverantwoordelijke verwerkte persoonsgegevens wist of teruggeeft, en bestaande kopieën verwijdert;

- de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de Verordening rondom het inzetten van een verwerker worden nageleefd en die nodig is om audits mogelijk te maken;
- afspraken met betrekking tot sub-verwerkers maakt.

Bij de aanwijzing van iedere aanvullende of gewijzigde verwerker zal een verwerkersovereenkomst worden gesloten.
Bij het opzeggen van de rechtsbetrekking met een verwerker zal de met deze partij gesloten verwerkingsovereenkomst voor een periode worden bewaard die Boomzagerij- Boomrooierij-Rondhouthandel Sikko Polling B.V. in staat stelt om te beoordelen of de betreffende verwerker heeft voldaan aan zijn verplichtingen uit de verwerkersovereenkomst en de AVG.

De met de verwerkers gesloten verwerkersovereenkomsten zijn bijgevoegd als **bijlage.**

9. Het register van verwerkingsactiviteiten

Inleiding
Het register van verwerkingsactiviteiten is een opsomming van de belangrijkste informatie over de verwerkingen van persoonsgegevens. Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. dient dit register zelf bij te houden.

Het register is schriftelijke opgesteld en wordt bijgehouden in elektronische vorm.
In het register zijn de volgende onderdelen opgenomen:

- contactgegevens;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
- indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie. Indien hiervan gebruik wordt gemaakt zullen ook de documenten inzake de passende waarborgen worden vermeld;
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens zullen worden gewist;
- een verwijzing naar dit gegevensbeschermingsbeleid inzake de technische en organisatorische beveiligingsmaatregelen.

Voor de meest actuele versie van het gebruikte register van verwerkingsactiviteiten dient de elektronische versie te worden geraadpleegd. Dit register is toegankelijk via de cloudopslag van Polling Vastgoed.

NB: *In het register neemt u niét de daadwerkelijke persoonsgegevens van betrokkenen op! Het register geeft slechts door middel van een beschrijving inzicht in de verwerkingsactiviteiten. Het register bevat dus een beschrijving van de verwerkingsactiviteiten en niét de persoonsgegevens zelf.*

10. FG - functionaris voor gegevensbescherming

De Verordening kent een belangrijke rol toe aan de functionaris voor gegevensbescherming . De functionaris voor gegevensbescherming (FG) houdt intern toezicht op en adviseert over de toepassing en naleving van de Verordening door uw organisatie. Ook is de FG het aanspreekpunt voor de betrokkene. In een aantal gevallen is het aanstellen van een FG verplicht.
Sikko Polling B.V. is niet verplicht om een FG aan te stellen. Boomzagerij- Boomrooierij-Rondhouthandel Sikko Polling B.V. voldoet namelijk niet aan de daarvoor gestelde en hieronder opgenomen voorwaarden.

1. de onderneming is geen overheidsinstantie of overheidsorgaan;
2. de onderneming is niet hoofdzakelijk belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen.
3. de onderneming is niet hoofdzakelijk belast met verwerkingen die de grootschalige verwerking van bijzondere categorieën van persoonsgegevens en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten behelzen.
   Ook bestaan de kernactiviteiten van de onderneming niet uit het grootschalig verwerken van bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard.

11. Gegevensbeschermingseffectbeoordeling (DPIA)

Wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, dan dient er voorafgaand aan de verwerking een zogenaamde gegevensbeschermingseffectbeoordeling uitgevoerd te worden. Dit noemt men ook wel een Data Protection Impact Assessment (DPIA) of Privacy Impact Assessment (PIA).

Een gegevensbeschermingseffectbeoordeling is een beoordeling van de effecten van een voorgenomen verwerkingsactiviteit op de bescherming van persoonsgegevens en de rechten en vrijheden van betrokkenen. Een gegevensbeschermingseffectbeoordeling is een instrument om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt, de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op basis hiervan worden maatregelen getroffen om deze effecten voor betrokkenen te voorkomen of te verkleinen.
In het algemeen toont men met een gegevensbeschermingseffectbeoordeling aan dat aan de vereisten van de Verordening wordt voldaan voor die verwerkingsactiviteit.

Uitleg 'hoog risico'
Volgens de Verordening is er in ieder geval sprake van een hoog risico wanneer men:

- geautomatiseerd systematisch en uitgebreid persoonlijke aspecten evalueert, waaronder begrepen profilering, en op basis daarvan besluiten neemt met rechtsgevolgen voor de betrokkene, of die de betrokkene anderszins in aanzienlijke mate treffen;
- op grote schaal bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard verwerkt;
- grootschalig en stelselmatig mensen volgt in openbaar toegankelijke ruimten (bijvoorbeeld door middel van cameratoezicht).

Dit is echter geen uitputtende lijst. Hoewel de Verordening deze drie situaties specifiek noemt, dient voor alle situaties met een mogelijk hoog risico voor betrokkenen een gegevensbeschermingseffectbeoordeling te worden uitgevoerd. Om te bepalen of er mogelijk sprake is van een hoog risico hanteren de toezichthouders de onderstaande vuistregel. Er is sprake van een hoog risico wanneer de voorgenomen verwerking aan twee of meer van de onderstaande negen criteria voldoet:

1. evaluatie van personen of scoretoekenning;
2. geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg;
3. stelselmatige monitoring;
4. gevoelige gegevens of gegevens van zeer persoonlijke aard;
5. op grote schaal verwerkte gegevens;
6. matching of samenvoeging van datasets;
7. gegevens met betrekking tot kwetsbare betrokkenen;
8. innovatieve toepassing van nieuwe technologische of organisatorische oplossing;
9. blokkering van een recht, dienst of contract.

De Europese privacytoezichthouders hebben aangegeven dat als vuistregel gehanteerd kan worden dat een DPIA uitgevoerd moet worden wanneer de verwerking aan 2 of meer van de onderstaande 9 punten voldoet:

1. U beoordeelt mensen op basis van persoonskenmerken (voorbeeld: een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt).
2. U neemt geautomatiseerde beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben (voorbeelden: geautomatiseerde verkeersboetes, geautomatiseerde beslissingen van overheidsinstanties, zoals de Sociale Verzekeringsbank die op een AOW-aanvraag beslist).
3. U houdt zich bezig met stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht.
4. U verwerkt gevoelige persoonsgegevens het gaat hierbij om bijzondere categorieën van persoonsgegevens, maar ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens).
5. houdt zich bezig met grootschalige gegevensverwerkingen. Of verwerkingen grootschalig zijn, hangt af van de hoeveelheid mensen van wie gegevens worden verwerk, de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt, de tijdsduur van de gegevensverwerking en de geografische reikwijdte van de gegevensverwerking.
6. U combineert databases met persoonsgegevens met elkaar of koppelt databases met gegevens aan elkaar.
7. U verwerkt persoonsgegevens over kwetsbare personen (er is vaak sprake van een ongelijke machtsverhouding tussen u en de betrokkene. Denk aan werknemers, kinderen en patiënten).
8. U maakt gebruik van nieuwe technologieën (bijvoorbeeld vingerafdruksystemen en gezichtsherkenning t.b.v. toegangscontrole, een automatic numberplate recognition camera of “internet of things” applicaties die een grote impact kunnen hebben op het dagelijks leven en de privacy van mensen).
9. De verwerking van persoonsgegevens kan leiden tot het niet kunnen uitoefenen van een recht, het niet gebruik kunnen maken van een dienst of het niet kunnen afsluiten van een contract (voorbeelden: gegevensverwerkingen die plaatsvinden in de openbare ruimte en die mensen niet kunnen vermijden, een bank die de kredietwaardigheid van klanten toetst om te bepalen of zij een lening krijgen).

Op basis van het vorenstaande is Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. **niet** verplicht om een gegevensbeschermingseffectbeoordeling uit te voeren. Sikko Polling B.V. voldoet namelijk niet aan de daarvoor gestelde en hieronder opgenomen voorwaarden:

1. de onderneming is geen overheidsinstantie of overheidsorgaan;
2. de onderneming voert geen verwerkingen uit die (waarschijnlijk) een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.

12. Privacy by Design en Privacy by Default

Inleiding
Een nieuw uitgangspunt in de Verordening is het beginsel van privacy door ontwerp en door standaardinstellingen, in de praktijk vaak aangeduid met de Engelse benamingen Privacy by Design en Privacy by Default. Privacy door ontwerp en door standaardinstellingen houdt kort gezegd in dat de privacy en gegevensbescherming meegenomen moet worden als eisen bij de ontwikkeling van nieuw beleid of het ontwerp van nieuwe systemen waarmee persoonsgegevens worden verwerkt. Voor Sikko Polling B.V. betekent dit dat ervoor gezorgd dient te worden dat een zo klein mogelijke inbreuk op de persoonlijke levenssfeer wordt gemaakt bij de verwerkingsactiviteiten.

Het uitgangspunt van privacy door ontwerp en door standaardinstellingen is in de Verordening neergelegd als een concrete plicht voor de verwerkingsverantwoordelijke. Welke technische en organisatorische maatregelen er genomen moeten worden om invulling te geven aan het uitgangspunt van privacy door ontwerp en door standaardinstellingen is afhankelijk van het concrete geval. Bij het bepalen van de verwerkingsmiddelen en de verwerking moet rekening gehouden worden met de volgende elementen:

- de stand van de techniek;
- de uitvoeringskosten;
- de aard, omvang, context en het doel van de verwerking;
- de risico's voor de betrokkene.

Deze elementen bepalen gezamenlijk welke technische en organisatorische maatregelen genomen moeten worden om de gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren en de nodige waarborgen in te bouwen ter naleving van de eisen uit de Verordening. Met andere woorden: de maatregelen die genomen moeten worden moeten in verhouding staan tot de risico's en redelijk zijn met het oog op de stand van de techniek en de uitvoeringskosten die gemaakt moeten worden om de maatregelen te implementeren.

Bij het ontwerpen van de systemen en processen van de onderneming zijn de volgende ontwerpstrategieën gehanteerd:

1. Data georiënteerde ontwerp strategieën
    - Minimaliseer: Beperk zoveel mogelijk de verwerking van gegevens. Selecteer voor het verzamelen. Verwijder wanneer mogelijk.
    - Scheid: Scheid persoonsgegevens zoveel mogelijk van elkaar en werk zo gedistribueerd mogelijk.
    - Abstraheer: Aggregeer tot het hoogst mogelijke niveau. Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.
    - Bescherm/maak onherleidbaar: Voorkom dat gegevens openbaar worden. Beveilig gegevens. Verbreek waar mogelijk de link tussen personen en gegevens (anonimiseer en pseudonimiseer).

2. Proces georiënteerde ontwerp strategieën
    - Informeer: Informeer gebruikers over de verwerking van hun persoonsgegevens.
    - Geef controle: Geef gebruikers controle over de verwerking van hun persoonsgegevens.
    - Dwing af: Stel een privacybeleid op en dwing dit af met technische en organisatorische middelen.

- Toon aan: Toon aan dat op een privacyvriendelijke wijze persoonsgegevens worden verwerkt. Verzamel logs, doe audits en rapporteer.

De interne beleidsmaatregelen die Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. genomen heeft en de technische maatregelen die zijn toegepast zijn opgenomen in dit gegevensbeschermingsbeleid in hoofdstuk 13, beveiliging.

13. Beveiliging

Inleiding
De verwerker van persoonsgegevens is verplicht om passende technologische en organisatorische maatregelen te nemen ter bescherming van deze persoonsgegevens. ‘Passend’ houdt in dat het beschermingsniveau moet worden aangepast aan de gevoeligheid en mogelijke bedreiging voor de persoonlijke levenssfeer van de betrokkene. Welke maatregelen van de verantwoordelijke en zijn/haar verwerker kunnen worden gevergd is afhankelijk van vele factoren. De volgende punten spelen hierbij een rol:

- de aard van de persoonsgegevens die worden verwerkt;
- de omvang van de verwerking van persoonsgegevens;
- de doeleinden waarvoor verwerking plaatsvindt;
- de mogelijke dreigingen;
- de ernst van de gevolgen die een beveiligingsincident zou kunnen hebben;
- de kans dat deze gevolgen zich zouden verwezenlijken;
- de stand van de techniek;
- de kosten van tenuitvoerlegging van beveiligingsmaatregelen; en
- de omvang en financiële mogelijkheden van de organisatie.

BELEID
Om zorg te dragen voor een passende technische beveiliging heeft Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. een specialist opdracht gegeven voor advisering, begeleiding en implementatie van technische beveiligingsmaatregelen. De uitkomsten hiervan zijn opgenomen in het rapport technische maatregelen. Dit rapport is bijgevoegd als bijlage bij dit beleidsdocument.
Opmerking: klopt dit?

De door Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. toegepaste technische maatregelen zijn onder andere: Opmerking: klopt dit?

- pseudonimisering en versleuteling van persoonsgegevens;
- firewalls;
- virusscanners;
- software tegen malware-aanvallen;
- het periodiek maken van back-ups;
- software waarmee de verantwoordelijke of verwerker wordt geattendeerd op het dreigende verstrijken van een bewaartermijn.

De door Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. toegepaste organisatorische maatregelen zijn:

1. Bestuurders en bewustzijn

De ondernemingheeft duidelijke protocollen en procedures opgesteld voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging.
Het bestuur is voldoende bewust van de verplichtingen uit de AVG.

2. Fysieke maatregelen

Er wordt gebruik gemaakt van specifieke fysieke beveiligingsmaatregelen, passend bij de aard van de te beschermen informatie:

- Bestuursleden bergen vertrouwelijke informatie na gebruik goed op en apparatuur wordt, indien niet gebruikt, vergrendeld;
- Er zijn passende blusmiddelen die periodiek worden gecontroleerd;
- Apparatuur, waarop informatie wordt verwerkt of is opgeslagen, wordt conform voorschriften van de leverancier onderhouden;
- het bewaren van persoonsgegevens op servers in een afgesloten ruimte;
- het bewaren van papieren dossiers in afsluitbare kasten;
- Informatiedragers inclusief papieren documenten met vertrouwelijke informatie, die niet meer nodig zijn, worden vernietigd (bijvoorbeeld door middel van een shredder) of afgevoerd door een gespecialiseerd vernietigingsbedrijf;
- Alleen onomkeerbaar geschoonde apparatuur mag worden hergebruikt door derden.

3. Logische toegang

- Bestuursleden delen hun wachtwoorden met niemand en zorgen ervoor dat ze aan niemand bekend kunnen raken;
- Bij wijziging van rollen worden de toegangsrechten zo nodig aangepast;
- Bij beëindiging van de inzet van een bestuurder worden toegangsrechten ingetrokken;
- Periodiek worden uitgegeven toegangsrechten gecontroleerd op correctheid, zodat onterecht uitgedeelde rechten kunnen worden ingetrokken.

Risico's

Deze maatregelen zijn gebaseerd en afgestemd op de volgende vastgestelde risico's voor de betrokkene. Risico's voor betrokkenen doen zich met name voor in situaties waar er sprake is van verlies, vernietiging, wijziging, ongeoorloofde verstrekking of ongeoorloofde toegang tot persoonsgegevens. Bij risico's voor betrokkenen moet gedacht worden aan lichamelijke, materiële of immateriële schade.

Van dergelijke risico's is voornamelijk sprake wanneer de verwerking kan leiden tot:

- discriminatie;
- identiteitsdiefstal of -fraude;
- financiële verliezen;
- reputatieschade;
- verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
- ongeoorloofde ongedaanmaking van pseudonimisering;
- enig ander aanzienlijk economisch of maatschappelijk nadeel.

Een verhoogd risico wordt in ieder geval aangenomen wanneer:

- de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen;
- wanneer persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt;
- bij de verwerking van genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen;
- wanneer persoonlijke aspecten worden geëvalueerd, om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;

- wanneer persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt; of
- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

De ondernemingheeft dit risico objectief vastgesteld, wat inhoudt dat een externe partij dit risico zo zou vaststellen. Naar het oordeel van Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. gaat de verwerking niet gepaard met een hoog risico.

Tussentijdse evaluatie van de maatregelen

De getroffen beveiligingsmaatregelen dienen gedurende de gehele looptijd van de verwerking passend te zijn. Dit betekent dat er, met name bij verwerkingen die langere tijd voortduren, periodiek geëvalueerd dient te worden of de genomen beveiligingsmaatregelen nog steeds passend zijn. Wanneer bijvoorbeeld door technische ontwikkelingen cybercriminelen nieuwe methoden tot hun beschikking krijgen om uw beveiligingsmaatregelen te ondermijnen, dan moet de beveiliging hierop aangepast worden.
Om die reden zal het bestuur van de onderneming periodiek evalueren. Onder periodiek wordt verstaan in ieder geval jaarlijks en zo nodig vaker indien daartoe aanleiding bestaat.

14. Datalekken en procedure omgang met datalekken.

De Verordening bevat een verplichting om onder omstandigheden een inbreuk in verband met persoonsgegevens (een datalek) mede te delen aan de Autoriteit Persoonsgegevens en de betrokkene. Een datalek kan voor betrokkenen grote gevolgen hebben, waaronder verlies van controle over hun persoonsgegevens, de beperking van hun rechten, discriminatie, identiteitsdiefstal of financiële verliezen. Het is dan ook van belang dat een datalek tijdig en op passende wijze wordt aangepakt. De verplichte mededeling aan de Autoriteit Persoonsgegevens en in voorkomende gevallen aan de betrokkene is daar een uitwerking van.

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. heeft een protocol opgesteld hoe intern dient te worden gehandeld in het geval van een beveiligingsincident waarbij mogelijk sprake is van een datalek. Het protocol datalekken is bijgevoegd als **bijlage.**

15. De waarborgen die worden gehanteerd bij de overdracht van gegevens buiten de Europese Unie

Het doorgeven van persoonsgegevens aan partijen/derden die buiten de Europese Economische Ruimte (EER) zijn gevestigd is beperkt onder de AVG. Bij een dergelijke doorgifte is Sikko Polling B.V. verplicht om de betrokkene te laten weten of dit land adequaat is verklaard door de Europese Commissie. Is zo'n besluit er niet, dan zal aangegeven moeten worden welke passende en geschikte waarborgen dit land dan biedt ter bescherming van persoonsgegevens, hoe hier een kopie van kan worden verkregen of waar deze kunnen worden geraadpleegd.

Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. doet zaken met bedrijven die in landen buiten de EER gevestigd zijn. Indien Sikko Polling B.V. persoonsgegevens doorgeeft aan externe partijen gevestigd buiten de EER en waar geen adequaat beschermingsniveau aanwezig is, blijft Boomzagerij- Boomrooierij- Rondhouthandel Sikko Polling B.V. toezicht houden op de verwerking van persoonsgegevens en maakt Sikko Polling B.V. gebruik van wettelijke doorgiftemechanismen om ervoor te zorgen dat de persoonsgegevens voldoende zijn beschermd. Voorbeelden hiervan zijn het gebruik van EU Standaard Contracten of contracteren met partijen gecertificeerd onder het EU-US Privacy Shield of daarvoor in de plaats te treden regelingen.

16. Autoriteit persoonsgegevens als toezichthouder

Inleiding
De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. Onder toezicht vallen diverse activiteiten, zoals onderzoek doen. De AP kan uit eigen beweging een onderzoek doen naar de naleving van de privacywetgeving. Dit heet ambtshalve onderzoek. De AP kan zo'n onderzoek bijvoorbeeld starten vanwege actuele gebeurtenissen of tips die de AP ontvangt over mogelijke overtredingen van de wet. Daarnaast kan de AP op verzoek van belanghebbenden (zoals burgers of belangenorganisaties) een onderzoek instellen.

Wat de criteria's zijn en hoe dit onderzoek er onder de AVG uit gaat zien zal de praktijk na 25 mei 2018 moeten uitwijzen. Sikko Polling B.V. verwacht dat dit overeenkomt met het onderzoek zoals dat door de AP onder de Wet bescherming persoonsgegevens plaatsvindt. Tot 25 mei 2018 zag een onderzoek door de AP er als volgt uit:

Criteria onderzoek
De AP hanteerde tot 25 mei 2018 de volgende criteria om te bepalen of er voldoende aanleiding is om onderzoek te doen:

- ernstige overtredingen;
- die structureel van aard zijn;
- die veel mensen treffen;
- waarbij de AP door de inzet van handhavingsinstrumenten effectief verschil kan maken;
- die vallen binnen de (jaarlijkse) aandachtspunten die de AP bekend heeft gemaakt.

Onderzoeksaanpak
Besloot de AP een ambtshalve onderzoek te starten, dan bepaalt de AP per situatie de aanpak en diepgang van het onderzoek. Dit kon uiteenlopen van een brief met het verzoek om informatie tot een onderzoek op locatie bij de onderzochte partij(en). Ook een steekproef op meerdere plaatsen in een sector was mogelijk.

In grote lijnen verliep een onderzoek van de AP als volgt:

1. onderzoek;
2. voorlopige bevindingen;
3. zienswijze;
4. definitieve bevindingen;
5. openbaarmaking;
6. handhaving.

Onderzoek
In deze fase verzamelde de AP alle benodigde informatie om te kunnen beoordelen of sprake is van een overtreding van de wet. De AP verzocht de betrokken partijen bijvoorbeeld om schriftelijk gegevens te overleggen.

Onderzoek ter plaatse
De AP kon ook besluiten om onderzoek uit te voeren op locatie bij de verantwoordelijke om een goed beeld te krijgen van de feitelijke situatie. Dit heette onderzoek ter plaatse. Het onderzoek kon zowel aangekondigd als onaangekondigd plaatsvinden.

Wanneer de handelswijze van de AP na 25 mei 2018 duidelijk wordt zal de onderneming een protocol opstellen indien daartoe aanleiding zal ontstaan.

Beleid
Totdat de werkelijke handelswijze van de AP duidelijk wordt zal het volgende beleid gelden:

Wanneer de AP (on)aangekondigd informatie bij de onderneming opvraagt dan zal een kopie van de volgende documenten aan de AP worden overlegd:

1. het gegevensbeschermingsbeleid
2. de bij het gegevensbeschermingsbeleid behorende bijlagen;
   - Register van verwerkingsactiviteiten;
   - Verwerkersovereenkomsten;
   - Protocol datalekken;
3. een kopie van de gedocumenteerde datalekken

17. Vaststelling en periodiek evaluatie

Dit beleid is vastgesteld op ……2018.

Directie:

…….

Evaluatie:

……

……

……

……

……

……

18. Bijlagen

Aan dit beleid zijn de volgende bijlagen gehecht:

Bijlage 1: Privacy statement
Bijlage 2: Protocol uitoefening rechten betrokkenen
Bijlage 3: Verwerkersovereenkomsten
Bijlage 4: Protocol datalekken